AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of Oregon

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Phones currently located at ATF Portland Field Office. 1201 NE Lloyd Blvd. Ste. 710, Portland, Oregon as described in Attachment A.

Case No. '19 -MC- 511

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Phones currently located at ATF Portland Field Office. 1201 NE Lloyd Blvd. Ste. 710, Portland, Oregon as described in Attachment A hereto.

located in the _____ District of Oregon, there is now concealed *(identify the person or describe the property to be seized)*:

The information and items set forth in Attachment B hereto.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 924(c)	Possession of firearm in furtherance of drug trafficking offense;
21 U.S.C. § 841(a)(1)	Distribution of cocaine.

The application is based on these facts:
See affidavit which is attached hereto and incorporated herein by this reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

NATHAN A. MILLER
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/13/2019

Judge's signature

City and state: (CITY), Oregon

JOLIE A. RUSSO, United States Magistrate Judge
Printed name and title

FILED 13 JUN '19 15:13 USDC-ORP

DISTRICT OF OREGON, ss: AFFIDAVIT OF NATHAN MILLER

Affidavit in Support of an Application for a Search Warrant for a Phone

I, Nathan Miller, being duly sworn, do hereby depose and state as follows:

Introduction and Agent Background

1. I am a Special Agent with the Bureau of Alcohol, Tobacco, Firearms, and Explosives, and have been since July 2014. My current assignment is to the Portland, Oregon Field Office. My training includes twenty-seven (27) weeks of ATF Special Agent Basic Training at the Federal Law Enforcement Training Center in Glynco, Georgia. As an ATF Special Agent, I am charged the responsibility of enforcing Federal firearms laws of the United States. I have participated in investigations involving firearms trafficking, National Firearms Act violations, unlawful firearms possession, and illegal narcotic trade, which often involves firearms. I have participated in investigations where the use of computers, smart phones, digital media, and the internet have been used in furtherance of crimes related to the illegal possession / trafficking of firearms and illegal narcotics.

2. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the search and examination of the following cellular devices (collectively Phones) are described in Attachment A hereto, and the extraction of electronically stored information from the Phones, as described in Attachment B hereto.

- Samsung J3 smartphone, in custody as ATF item 0008. (Hereinafter Phone 2)
- Samsung flip phone, in custody as ATF item 0009. (Hereinafter Phone 3)
- ZTE flip phone, in custody as ATF item 0010. (Hereinafter Phone 4)

- Apple iPhone, in custody as ATF item 0011. (Hereinafter Phone 1)
- Apple iPhone, in custody as ATF item 0012. (Hereinafter Phone 5)

3. The Phones are currently located and secured in evidence at the ATF Portland Field Office, located at 1201 NE Lloyd Boulevard, Suite 700, Portland, Oregon. In my training and experience, I know these Phones have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Phones first came into the possession of ATF.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers, interviews of witnesses, a review of records related to this investigation, communications with others who have knowledge of the events and circumstances described herein, and information gained through my training and experience.

Applicable Law

5. As set forth below, I have probable cause to believe and do believe that the items set forth in Attachment B constitute evidence and fruits of:

- Title 18 U.S.C. § 924(c)(1)(A), which makes it a crime for any person who, during and in relation to any crime of violence or drug trafficking crime for which the person may be prosecuted in a court of the United States, uses or carries a firearm, or who in furtherance of any such crime, possesses a firearm.

- Title 21 U.S.C. § 841(a)(1), which makes it a crime for any person knowingly or intentionally to manufacture, distribute, or dispense, or possess with intent to manufacture, distribute, or dispense, a controlled substance (cocaine).

Statement of Probable Cause

6. On February 25, 2019, a Washington County Sheriff's Office (WCSO) Deputy initiated a traffic stop near 20159 SW Tualatin Valley Highway, Beaverton, Oregon, on a green Hummer 2 (OR: 725DEZ) for failing to maintain a lane. The driver was identified as Luis Miguel Salvador Madrigal. A WCSO Narcotics K9 arrived minutes later and alerted to Madrigal's vehicle while the deputy who initiated the traffic stop was issuing a citation. When asked why the K9 would alert to his vehicle, Madrigal stated, "There is a lot of powder in the back seat." Madrigal was read his rights per *Miranda.* When asked if he understood his rights, Madrigal responded in the affirmative. Deputies detained Madrigal and searched his vehicle, recovering approximately 283.6 grams of suspected cocaine.

7. Madrigal was interviewed on scene by WCSO Det. Weed. Madrigal consented to the search of his residence located at 20085 SW Rock Road, Beaverton, Oregon, but denied consent to search the phone located on his person (Phone 1). A large quantity of cash was additionally found on Madrigal's person. Madrigal said he sent a message to someone saying that he was stopped by police. Madrigal stated there was multiple firearms in his room, including an AK-47.

8. WCSO deputies responded to Madrigal's residence and observed a male, later identified as Ramiro Madrigal-Magana walk out of the house and look up and down the street. Madrigal-Magana returned back inside the house, and a female, Witness 1 ("W1") walked

outside and looked up and down the street. W1 walked back inside the house and Madrigal-Magana departed on foot carrying a bag. WCSO Deputies observed Madrigal-Magana standing in the street and attempted to stop him. Madrigal-Magana fled on foot and was apprehended.

9. Madrigal-Magana was read his rights in Spanish, and when asked if he understood, he responded in the affirmative. Madrigal-Magana gave consent to search the bag he carried out of the house. The same WCSO K9 responded to the scene and positively alerted to the bag. Deputies recovered 471.5 grams of suspected cocaine from the bag, and Phone 2 and Phone 3 from Madrigal-Magana's person.

10. Deputies contacted W2, W3, and W1 at the residence and informed them of the investigation concerning Madrigal and Madrigal-Magana. W1, W2 and W3 each consented to the search of the residence. Deputies recovered cash, 3.7 grams of suspected cocaine, and a Colt pistol, model MKIV, .38 caliber, SN: 70S04170 from the master bedroom associated with W1 and Madrigal-Magana. Deputies recovered the following from Madrigal's room:

- Ruger rifle, model 10-22, .22 caliber, SN: 125-07334, found behind bedroom door.
- FN pistol, model Five-Seven, 57 caliber, SN: 386346285, found on bed underneath pillow.
- Bushmaster rifle, model XM15-E2S, .223 caliber (with attached 37mm grenade launcher), SN: L122921, found behind bed.
- Izhmash shotgun, model Saiga-12, 12 gauge, SN: 12422737, found behind bed.
- Norinco rifle, model MAK90 Sporter, 7.62 caliber, SN: CW-19830, found behind bed.
- 5 grams of suspected cocaine, found in backpack.
- Multiple rounds of ammunition of assorted calibers found around the room.

- Phone 4, found on the floor of the room.
- Cash from the dresser drawer.

11. W1 stated to deputies she observed Madrigal-Magana go into Madrigal's room, retrieve a bag, and leave the residence, prior to deputies arriving.

12. In total, deputies seized 763.8 grams of suspected cocaine and $19,156.00 in cash. Madrigal and Madrigal-Magana were arrested. Madrigal was charged with Distribution of Cocaine. Madrigal-Magana was charged with Distribution of Cocaine, Unlawful possession of Fictitious ID, Felon in Possession of Firearm, and Interfering with a Police Officer.

13. On March 7, 2019, Madrigal was released from the Washington County Jail on bail for $500.00.

14. On April 29, 2019, Det. Weed obtained a search warrant for Phones 1-4. Data from Phones 1-4 were extracted by WCSO pursuant to the aforementioned search warrant. The search warrant permitted the search of the devices for evidence of Unlawful Delivery of Cocaine during the date range of February 1, 2019 through February 27, 2019.

15. On May 9, 2019, I received a copy of the phone data extract from Det. Weed, and he informed me the data had not been reviewed. I told Det. Weed I would search the data pursuant to the warrant and inform him of the findings.

16. On May 17, 2019, I received information from WCSO that Madrigal was taken into custody at his court appearance at the Washington County Circuit Court. I responded to the court and met with Madrigal. I read Madrigal his rights per *Miranda*, and when asked if he understood his rights, Madrigal responded in the affirmative. I informed Madrigal his case was adopted by ATF, and he would be transported to United States Marshal's Service custody. I

asked Madrigal if he had any property on his person. Madrigal told me he had his phone and wallet. I subsequently seized Madrigal's phone (Phone 5) and informed him a search warrant would be written for the device. I told Madrigal the search of the device could be expedited if he unlocked the device, but Madrigal denied to unlock the phone.

17. On June 3, 2019, I opened the data extracts of Phones 1-4 with UFED Physical Analyzer program version 7.17.1.1. I began to review the information extracted on Phone 1 by looking at the photos and videos. I noticed multiple photos and videos of suspected narcotics possession by Madrigal. I reviewed the time stamp for the photos to assure they were in the scope of the warrant and noted they were dated as early as September 2018 (outside the scope of the warrant). I additionally saw multiple photos and videos that appeared to be firearms related that were also not included within the scope of the warrant. I checked the device to see when the earliest messages or phone calls occurred to ascertain an approximate date of activation. The date of activation on the device appeared to be in December 2017. I subsequently ceased my search pending a new search warrant that included an extended date range and firearms possession.

18. I subsequently viewed the data extracts for Phones 2-4 only to obtain information on the suspected activation date for reference on a new warrant. I found the earliest activation date was on Phone 3, which appeared to be activated in November 2017.

20. Based on my training and experience I know people involved in the unlawful acquisition and distribution of narcotics and/or firearms have the need to communicate with other persons in order to facilitate their illegal activities. This communication takes place between the seller and purchaser of narcotics and/or firearms. Equipment frequently used by

individuals who facilitate the sale of narcotics and/or firearms includes cell phones. I know people involved in narcotics and/or firearms distribution often document their possession and use of narcotics and firearms via videos, pictures, and messages on their cellular devices. I also know people involved in narcotics and/or firearms distribution utilize multiple cell phones or "burner" phones to conceal their illegal activity from law enforcement.

21. Based on my training and experience, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; recording, storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet,[1] including the use of apps.[2] Wireless telephones may also include a global positioning system ("GPS") technology for determining the location of the device.

---

[1] The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

[2] Apps is an abbreviation for applications. An app is a self-contained program or piece of software designed to fulfill a particular purpose. An app can run on the Internet, on a computer, on a cell phone, or on other electronic devices.

22. Based on my training, experience, and research, I know that the Phones have capabilities that allow them to serve as wireless telephone, digital camera, and portable media player. In my training and experience, examining data stored on wireless telephones can uncover, among other things, evidence that reveals or suggests who possessed or used the phone, how the phone was used, and the purpose of its use.

23. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant but also forensic evidence that establishes how the Phones were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on the Phones because, based on my knowledge, training, and experience, I know:

a. Phones can store information for long periods of time, including information viewed via the Internet. Files or remnants of files can be recovered with forensic tools months or even years after they have been downloaded onto a phone, deleted, or viewed via the Internet. Electronic files downloaded to a phone can be stored for years at little or no cost. When a person "deletes" a file, the data contained in the file does not actually disappear, rather that data remains on the phone until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the phone that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, the operating system may also keep a record of deleted data.

b. Wholly apart from user-generated files, a phone may contain electronic evidence of how it has been used, what it has been used for, and who has used it. To give a few

examples, this forensic evidence can take the form of operating system configurations, artifacts from operating systems or application operations, and file system data structures.

c. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

d. Data on a phone can provide evidence of a file that was once on the phone but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Systems can leave traces of information on a phone that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the phone that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, including SD cards or other flash media, and the times the phone was in use. File systems can record information about the dates files were created and the sequence in which they were created.

e. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

f. A person with appropriate familiarity with how a phone works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the phone was used, the purpose of its use, who used it, and when.

g. The process of identifying the electronically stored information necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data

stored on a phone is evidence may depend on other information stored on the phone and the application of knowledge about how a phone functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in order to find evidence of how a phone was used, the purpose of its use, who used it, and when, the examiner may have to establish that a particular thing is not present on the phone.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Phones consistent with the warrant. The examination may require authorities to employ techniques, including imaging the Phones and computer-assisted scans and searches of the Phones that might expose many parts of the device to human inspection in order to determine whether it constitutes evidence as described by the warrant.

25. The initial examination of the Phones will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

26. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Phones or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without

authorization from the Court. Law enforcement personnel may continue to examine files or data falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

27. If an examination is conducted, and it is determined that a phone does not contain any data falling within the ambit of the warrant, the government will return the phone to its owner within a reasonable period of time following the search and will seal any image of the phone, absent further authorization from the Court.

28. The government may retain the Phones as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Phones and/or the data contained therein.

29. The government will retain a forensic image of the Phones for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

30. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Conclusion

31. Based on the foregoing, I have probable cause to believe, and I do believe, that the Phones described in Attachment A contain evidence and fruits of violations of; Title 18 U.S.C. § 924(c)(1)(A), possession of firearm in furtherance of drug trafficking offense, and Title 21 U.S.C. § 841(a)(1), distribution of cocaine, as set forth in Attachment B. I therefore request that the Court issue a warrant authorizing a search of the Phones described in Attachment A for the items listed in Attachment B and the seizure and examination of any such items found.

32. Prior to being submitted to the Court, this affidavit, the accompanying application, and the requested search warrant were all reviewed by Assistant United States Attorney (AUSA) Greg Nyhus, and AUSA Nyhus advised me that in his opinion the affidavit and application are legally and factually sufficient to establish probable cause to support the issuance of the requested warrant.

NATHAN MILLER
ATF Special Agent

Subscribed and sworn to before me this 13th day of June 2019.

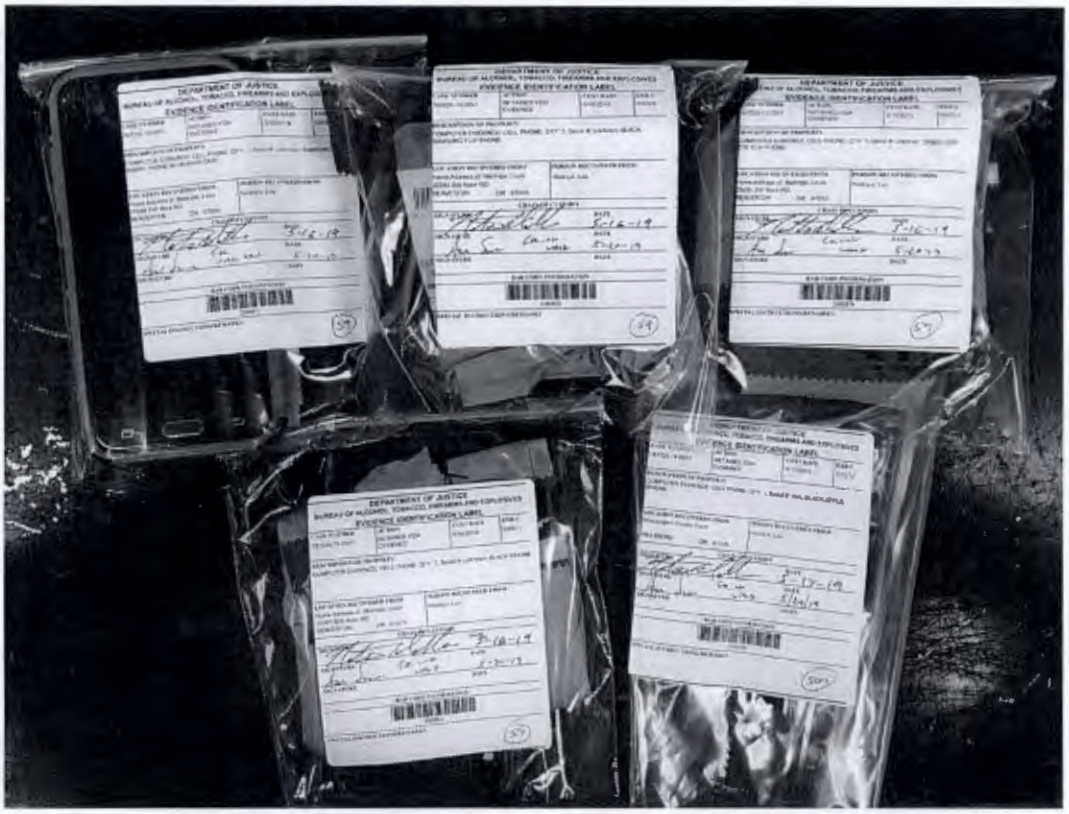
JOLIE A. RUSSO
United States Magistrate Judge

ATTACHMENT A

Phones to Be Searched

The phones to be searched:

1. Samsung J3 smartphone, in custody as ATF item 0008.
2. Samsung flip phone, in custody as ATF item 0009.
3. ZTE flip phone, in custody as ATF item 0010.
4. Apple iPhone, in custody as ATF item 0011.
5. Apple iPhone, in custody as ATF item 0012.



The phones are currently in the secure evidence locker at the ATF Portland Field Office, located at 1201 NE Lloyd Boulevard, Suite 700, Portland, Oregon.

ATTACHMENT B

Items to Be Seized

1. All records on the Devices described in Attachment A that relate to violations of Title 18 U.S.C. §§ 924(c)(1)(A), and Title 21 U.S.C. § 841(a)(1); and involve Luis Miguel Salvador Madrigal and Ramiro Madrigal-Magana since approximately December of 2017 including:

a. Evidence relating to illegal possession of firearms and narcotics.

b. Types, amounts, and prices of firearms and narcotics possessed as well as dates, places, and amounts of specific transactions.

c. Information related to sources of firearms and narcotics (including names, addresses, phone numbers, or any other identifying information).

d. Bank records, checks, credit card bills, account information, and other financial records indicating firearms and narcotics acquisition.

e. Bank records, checks, credit cards, account information and other financial records indicating identity theft.

2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Internet, including:

a. Records of Internet Protocol addresses used.

b. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses.

c. Records of data storage accounts and use of data storage accounts.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

Search Procedure

5. The examination of the Devices may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Devices to human inspection in order to determine whether it is evidence described by the warrant.

6. The initial examination of the Devices will be performed within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If the government needs additional time to conduct this review, it may seek an extension of the time period from the Court within the original 120-day period from the date of execution of the warrant. The government shall complete this review within 180 days of the date of execution of the warrant. If the government needs additional time to complete this review, it may seek an extension of the time period from the Court.

7. If, at the conclusion of the examination, law enforcement personnel determine that particular files or file folders on the Devices or image do not contain any data falling within the scope of the warrant, they will not search or examine those files or folders further without authorization from the Court. Law enforcement personnel may continue to examine files or data

falling within the purview of the warrant, as well as data within the operating system, file system, software application, etc., relating to files or data that fall within the scope of the warrant, through the conclusion of the case.

8. If an examination is conducted, and it is determined that the Devices do not contain any data falling within the ambit of the warrant, the government will return the Devices to its owner within a reasonable period of time following the search and will seal any image of the Devices, absent further authorization from the Court.

9. The government may retain the Devices as evidence, fruits, contraband, or an instrumentality of a crime or to commence forfeiture proceedings against the Devices and/or the data contained therein.

10. The government will retain a forensic image of the Devices for a number of reasons, including proving the authenticity of evidence to be used at trial, responding to questions regarding the corruption of data, establishing the chain of custody of data, refuting claims of fabricating, tampering, or destroying data, and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.